IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application No.	: 10/767,454	Confirmation No.	: 3942
First Named Inventor	: Richard C.BEESLEY		
Filed	: January 30, 2004		
TC/A.U.	: 2151		
Examiner	: Khanh Q. Dinh		
Docket No.	: 038819.53225US		
Customer No.	: 23911		
Title	: Method for Secure Communication Over a Public Data Network via a Terminal that is Accessible to Multiple Users		

REVISED APPEAL BRIEF

Mail Stop Appeal Brief - Patents **February 8, 2008**
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This Revised Appeal Brief is submitted pursuant to a Notice of Non-Compliant Appeal Brief mailed January 8, 2008 regarding the above-identified U.S. patent application. The original Appeal Brief was submitted on October 9, 2007. Accordingly, both the original Appeal Brief and this Revised Appeal Brief are timely submitted.

I. REAL PARTY IN INTEREST

This application has been assigned by the inventors to Roke Manor Research Limited, a UK corporation. Accordingly, the real parties and interests to the present appeal are the named inventors and Roke Manor Research Limited.

II. RELATED APPEALS AND INTERFERENCES

There are no other appeals or interferences known to Appellants, to Appellants' legal counsel or to the Assignee, which will directly affect or be directly affected by or having a bearing the Board's decision in this appeal.

III. STATUS OF CLAIMS

Claims 1-5 and 7-12 are currently pending in this application. In the amendment dated June 30, 2006, claims 13-24 were cancelled, as being drawn to a non elected invention, and in addition, claim 6 was cancelled and its substance incorporated into claim 1. All of the remaining claims have been rejected on prior art grounds. Accordingly, the status of all claims in this proceeding is as follows:

Claims 1-5 rejected, and being appealed.

Claims 6 cancelled.

Claims 7-12 rejected, and being appealed.

Claims 13-24 cancelled.

Appellants hereby seek reversal of the final rejection of claims 1-5 and 7-12.

IV. STATUS OF AMENDMENTS

Three amendments have been submitted in respect to the present application, dated May 1, 2006, June 30, 2006, and January 30, 2007, respectively. All such amendments have been entered. In addition, Applicants submitted a reply dated December 27, 2005, which did not amend the claims. That reply was considered in the Office Action dated January 30, 2006. No amendments have been submitted subsequent to the final Office Action dated April 9, 2007.

V. SUMMARY OF THE CLAIMED SUBJECT MATTER

The present invention is directed to an arrangement which avoids the possibility that sensitive data may be left on a publicly accessible user terminal after a network browsing session. The invention is thus important in situations, such as internet cafes, where one person may use a terminal and enter sensitive data (for example, passwords and credit card numbers). In such circumstances, the possibility exists that a second user may later be assigned to the same terminal, and would be able to discover and misuse the sensitive data, which is stored as a matter of course in the web browser which is resident on that terminal.

For example, a scenario in which residual data from an internet browsing session is left on a public PC is described at page 7 of the specification, in

connection with Figure 1. As shown in Figure 1, a public PC 1 such as might be found in an internet café, for example, comprises a hard disk 2 and a web browser 3. A first user of this multi user terminal may wish to make an online purchase of books, and for this purpose, launches the web browser 3 and enters the URL of the homepage of an online book vendor. (Specification, Page 7, lines 5-12.) The web browser thus accesses a remote server 4 of the vendor, via the internet. (Page 7, lines 13-15.)

The web browser 3, which is resident on the publically available terminal 1 automatically stores the URL in a browser history file on the hard disk 2. In the scenario discussed in the specification, the user has a pre-existing account with the vendor, and to access that account, he or she inputs a registered account user name and password to the browser 3 which stores this information on the hard disk 2. (Page 7, lines 13-23.) In order to complete the purchase, the user enters his or her credit card details into a form in a checkout page, and causes the browser to transmit this information to the web server 4. Once again, the browser automatically stores this information to a file on the hard disk 2. (Page 8, lines 1-8.)

When the user completes his or her use of the public terminal 1, and exits the internet café, the URL's of the visited web pages, the web pages themselves, the user name, password and credit card details of the user are all stored on the hard disk 2. (Page 8, lines 9-12.)

Subsequently, another individual enters the internet café and is allocated to the same PC 1. The subsequent user browsers the hard disk 2, and by performing an analysis of the web browser cache and history discovers the websites the user looked at, and his or her user name and password. This subsequent user is then able to logon to the vendors website and masquerade as the user. He or she may also be able to change the registered mail and email addresses of the user account and of course may misuse the credit card information by placing book orders. (Page 8, lines 14-23.)

The difficulty described above arises, because, due to the performance benefits of caching information, in virtually all web browsers the function for caching information such as described above is enabled by default. However, it is not within the ability of many users to disable this function, and in some software packages, it may not be possible to turn off every data gathering option. (Page 9, lines 1-9.) For example, as discussed at page 9, line 9 of the specification, internet explorer requires at least a one megabyte webpage cache, and some of the cache files are shared by Windows, so that the operating system "locks" the files, preventing deletion and removal of the information.

As discussed in the specification starting at page 10, line 8 and continuing through page 13, line 15, the present invention provides a solution to this problem by providing a remotely-accessible web browsing software, which a user may know and trust not to store sensitive data on the user terminal. In

particular, the user may use the terminal standard network to access a remote server to download the trusted web browsing software, and then use the (downloaded), trusted web browsing software to carry out transactions which involve the entry of sensitive data. (Page 10, lines 8-17.) When the user has finished using the terminal, he may close the trusted web browsing software, and thereby disconnect from the remote server. Because the downloaded browsing software is known to the user to have been configured to browse the internet without caching or otherwise storing data on the hard disk of the PC, the user can be secure in the knowledge that no sensitive data remains on that terminal, and that any later user would be able to discover only that the first user had accessed the remote server and downloaded a web browsing software.

A representative scenario according to the invention is discussed in the specification, at page 10, line 18 through page 12, line 23, and illustrated in Figure 2 of the drawings. In this scenario, the PC 1 is again located in publically accessible location, such as an internet café, and comprises a hard disk 2 with a web browser 3. As in the previous scenario, the user wishes to make an online purchase of books from an online vendor having a server 4. (Page 10, line 18 – Page 11, line 3.)

However, according to the invention, rather than immediately accessing the online vendor via the web browser 3 which is present on the local publically accessible PC 1, the user first inputs into the web browser 3 the URL of a trusted

website located on a second server 5 , and downloads from that website a trusted secure web browser 6, which has been configured to browse the internet without caching or otherwise storing data on the hard disk 2 of the PC 1. (In a preferred embodiment, the secure web browser 6 is JAVA applet.) (Page 11, lines 6-12.) As indicated, at page 11, line 13, the web browser 3 retrieves the secure web browser 6 via the internet and displays it within the main window of the web browser 3. (Page 11, lines 13-15.)

According to the invention, the user inputs the URL of the on line vendor into the secure web browser 6, which is now running within the web browser 3. (Page 11, lines 19-21.) All communication with the URL in question, however, is conducted by the secure web browser 6, whose configuration insures that neither the URL of the vendor nor the homepage itself are stored on the hard disk. Moreover, when the user accesses his or her account and inputs a registered account user name, password and credit card information, this information is not stored on the hard disk 2 of the PC 1. (Page 12, lines 13-18.)

After the user completes his or her web browsing and exits the internet café, he or she may be sure that neither the URL's of the visited web pages, the web pages themselves, nor his or her user name , password or credit card details have been saved on the hard disk 2. (Page 12, lines 19-23.) Indeed the only information which would remain on the hard disk 2 is the URL of the server 5 from which the secure browser software was downloaded. (Page 13, lines 1-5.)

Accordingly, it no longer possible for a subsequent user of the same publicly available terminal to obtain access to the confidential information of a previous user, as is the case with the prior art, described above. Indeed, the only information that such a subsequent user could find would be the URL of the visited webpage on the server 5 and downloaded a JAVA web browser applet. (Page 13, lines 3-5.)

In compliance with the requirement of the second sentence of 37 C.F.R. §41.37(c)(1)(v), Appellants note that none of the claims present in this application contains any means plus function or step plus function within the meaning of 35 U.S.C. §112, 6th paragraph.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Claims 1-5 and 7-12 have been rejected under 35 U.S.C. §102(b) as anticipated by Araujo et al. (published U.S. Patent Application 2003/0191799).

VII. ARGUMENT

As noted previously, the present invention provides a simple solution to a recurrent problem which exists whenever a user accesses the internet via a publicly available terminal (such as in an internet café,) and enters sensitive information into the system. As noted previously, for this purpose, according to the invention the user uses the existing web browser which is resident on the

publicly accessible terminal only to download a different web browser via the internet, with the latter web browser being configured such that is does not store any of the user's confidential data on the hard drive of the PC. Araujo et al., on the other hand, provides a different solution to a very different problem: in particular, it provides a way to securely connect a PC to a server for secure data access across different applications using a web browser's built in secure socket layer (SSL). Nowhere does Araujo et al., deal with the problem of maintaining security of the local terminal with respect to caching of files, in the manner described above.

Araujo et al. addresses the problem of users who are remote from their office, but wish to access a range of stored data and applications that are not present on their own local terminal, but which are available to them at a remote location. Rather than having to install and maintain a full range of desired applications on each computer terminal, and to ensure that all data is synchronized between the various computers which the user may access, Araujo et al. provides a network solution in which the user accesses remotely available applications and data through a web browsing software that is resident on the local terminal. That is, the user uses the local terminal's standard web browsing software to contact a remote server. The user may then download a desired application, and remotely interact with data that resides on the remote server. The user will be able to access data and use applications as if his terminal was locally connected to an office network.

Araujo et al is unconcerned with the issue of whether entered data are subsequently stored on the user's local terminal or are accessible to subsequent users of the same terminal. Araujo et al allows desired application software to be downloaded to a user's terminal through use of a standard browser. It does not provide a trusted web browsing software which is remotely accessible for download and use on non-secure terminals, as in the present invention, but rather provides a virtual-office application for remote workers.

See, for example, Paragraphs [0029], [0030]; [0031]; [0060]; and [0064] (lines 21-28). While Araujo et al discloses remote access to applications, and the downloading of HTML files for graphical display purposes, (Paragraph [0064] lines 1-28), it contains no disclosure that suggests downloading trusted web browser software and using it at the local terminal, so that no confidential information is stored on the local hard drive. Rather the system uses the web browser 15 (Fig. 1) that is already present on the user terminal for all browser activity. See Paragraphs [0061] and [0064] lines 27-28.

RESPONSE TO CLAIM REJECTIONS

CLAIM 1:

Araujo et al contains no provision for "transmitting a request for web browsing software stored on the server to be downloaded to a terminal". Moreover, it also fails to teach or suggest any provision for "receiving web

browsing software at the terminal", or "using the web browsing software which has been downloaded to the terminal to communicate from the terminal over the public network". Rather, as noted previously, in Araujo et al. all web browsing via the terminal in question is performed using the web browser 15 which is resident on the terminal itself, thereby leaving open the possibility of storing sensitive personal information.

Finally, Araujo et al also contains no teaching that downloaded web browsing software (of which there is none discussed in Araujo et al) is configured such that user input data which is input to the web browsing software by a terminal user, or data which are received from the network at the terminal by the web browsing software, are transmitted to the network or presented to the user "without storing a record of the data at the terminal". In fact, given the software and hardware configuration disclosed in Araujo et al, there is nothing which would prevent such storage. Accordingly, a subsequent user of the terminal in question could obtain access to the former user's personal information, since it is stored on the terminal.

Claims 2-5 and 7-12 are allowable due to their dependency on Claim 1. However, Appellants offer the following comments regarding those claims.

CLAIM 2:

In the passage referred to in the Office Action, Araujo et al teaches that a Java applet is used to encode user input data, such as mouse clicks and keystrokes, into AIP protocol, and to pass control information into the SEP of Araujo et al. Appellants respectfully submit, however, that this does not indicate or suggest that a web software embodied as a Java applet is involved, or provided, in any way.

CLAIM 4:

Araujo et al discloses that software is downloaded by and runs within a browser (reference numeral 15 in Fig. 1), but not that the downloaded software is itself a web browsing software.

CLAIM 5:

Insofar as Appellants can determine, Araujo et al discloses no "further browsing software".

CLAIM 7:

Appellants submit that nothing in Fig. 2 suggests that anything is arranged to communicate "with the public data network via a web browser application running on a remote server".

CLAIM 8:

Appellants are unable to identify the subject matter referred to in Araujo et al, since Araujo et al is not arranged by numbered columns and lines.

CLAIMS 9-10:

Araujo et al does not disclose or suggest that no record of input data is stored at the terminal, or that data provided to the user is not stored on the terminal. As discussed at length in the present application, it is a standard feature of virtually all computers that copies of such data will be stored. Accordingly, in the absence of any indication to the contrary, the arrangement of Araujo et al. would include the local storage of input and requested data. Moreover, Araujo et al contains no teaching of how to avoid such storage.

In response to the last paragraph of 37 C.F.R. §41.37, Appellants note that none of the claims which are subject of the present Appeal contain any means plus function or step plus function limitation, as provided in 35 U.S.C. §112, sixth paragraph.

VIII. CONCLUSION

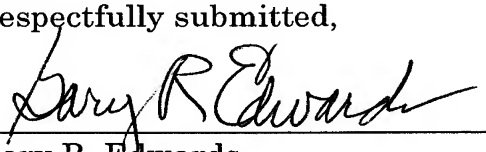
For the reasons set forth above, Appellants respectfully submit that claims 1-5 and 7-12 patentably distinguish over the cited Araujo et al reference and are

allowable. Accordingly, Appellants request that the board reverse the final rejection of claims 1-5 and 7-12.

This Appeal Brief is accompanied by the required appeal fee of $510. While this amount is believed to be correct. However, the Commissioner is hereby authorized to charge any deficiency, or credit any overpayment, to Deposit Account No. 05-1323, Docket No.: 038819.53225US.

.

Respectfully submitted,



Gary R. Edwards
Registration No. 31,824

CROWELL & MORING LLP
Intellectual Property Group
P.O. Box 14300
Washington, DC 20044-4300
Telephone No.: (202) 624-2500
Facsimile No.: (202) 628-8844
GRE:slw

4935513_1

CLAIMS APPENDIX

The following claims are the subject of this appeal.

Claim 1. A method of communicating over a public data network, the method comprising,

transmitting to a remote server on the network a request for web browsing software stored on the remote server to be downloaded to a terminal connected to the network;

receiving the web browsing software at the terminal; and

using the web browsing software which has been downloaded to the terminal to communicate from the terminal over the public data network; wherein, at least one of the following is true:

the web browsing software is configured such that user input data, which is input to the web browsing software by a user of the terminal, is transmitted into the network without storing a record of said input data at the terminal; and

data which are received from the network at the terminal by the web browsing software, at the request of the user, are presented to the user without storing a record of the data at the terminal.

Claim 2. A method according to claim 1, wherein the web browsing software is a Java Applet.

Claim 3. A method according to claim 1, wherein, the web browsing software is for communicating with web sites.

Claim 4. A method according to Claim 1, wherein the web browsing software is downloaded by and runs within a further communications application provided on the terminal.

Claim 5. A method according to claim 4, wherein the further communications application is a Web Browser.

Claim 6 (cancelled)

Claim 7. A method according to claim 1, wherein the web browsing software is arranged to communicate with the public data network via a Web Browser application running on a remote server.

Claim 8. A method according to claim 7 wherein the Web Browser application retrieves web pages from the network on behalf of the web browsing software, which receives the Web Pages in a non graphical format from the Web Browser application.

Claim 9. A method according to claim 1, wherein no copy of the data transmitted into the network or the data received from the network by the application is cached at the terminal or written to permanent memory at the terminal.

Claim 10. A method according to claim 1, wherein no record of a network address visited by the application from the terminal is stored at the terminal.

Claim 11. A method according to claim 10 wherein the network address is any of an IP address, domain name or a URL.

Claim 12. A server connected to a public data network, the server storing a communications application for downloading to a terminal connected to the network for use in the method of claim 1.

Claims 13.-24. (cancelled)

EVIDENCE APPENDIX

None.

RELATED PROCEEDINGS APPENDIX

None.